Summary of this Invention

Existing network systems based upon the client/server principle require on the server side the provision of open connection endpoints. The large number of server processes implies a large number of open connection endpoints. Each open connection endpoint is also a potential target for an ill-minded attacker. The present invention minimizes the risk of a break-in into a network with security critical data.

This problem is solved by minimizing the number of open connection endpoints, the temporary opening of selected connection endpoints and the random choice of the local identifications of the opened connection endpoints. Additionally, security critical data is isolated onto machines, which after build-up of predefined standing connections do not provide any open connection endpoints or establish further connections. This prohibits the build-up of uncontrolled connections to units storing security critical data and still offers the controlled access of the security critical data within the network. Security critical services are able to provide different protocols for different connections and allow the remote administration of the security critical data without granting normal clients access to administrative protocols or functions. Individual protocols or individual functions of individual protocols can be activated, deactivated, dynamically loaded or released into or out of the addressable memory of a security critical service during normal operation.